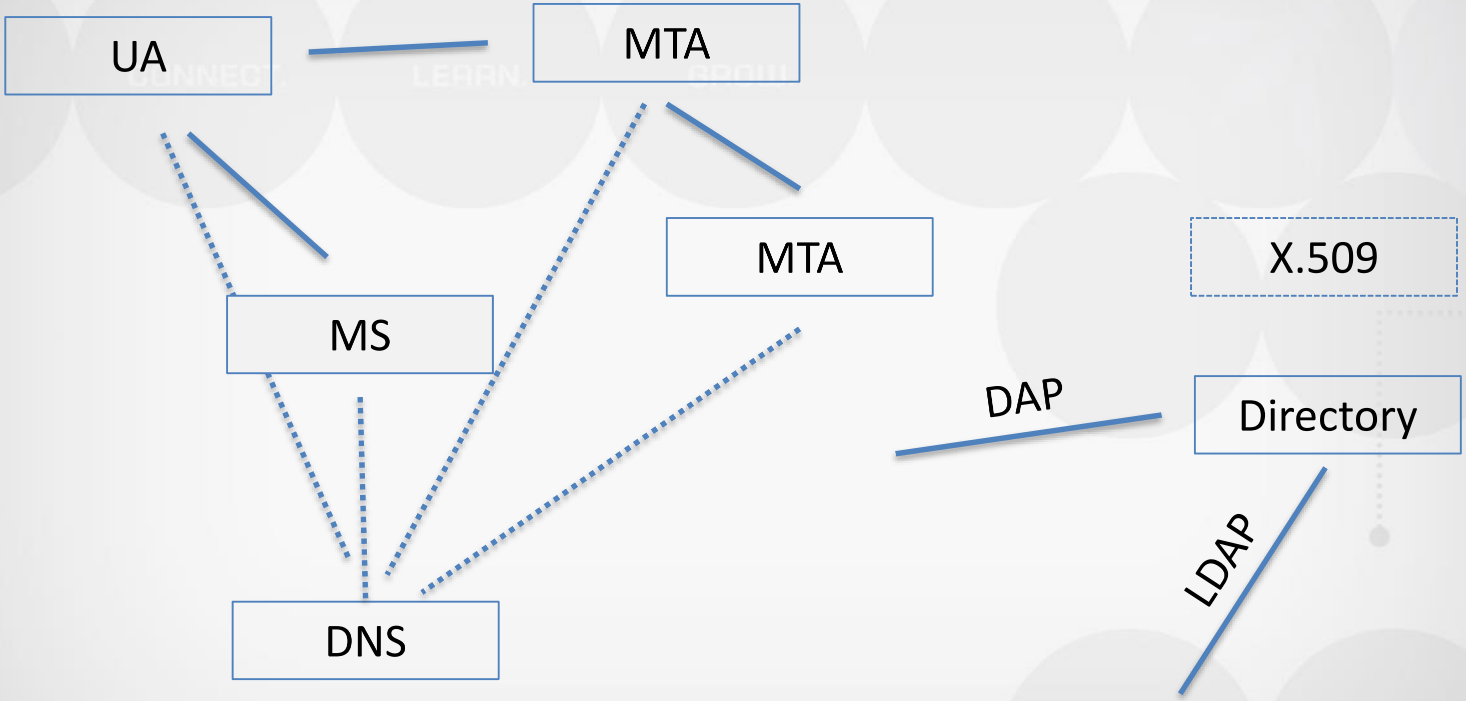
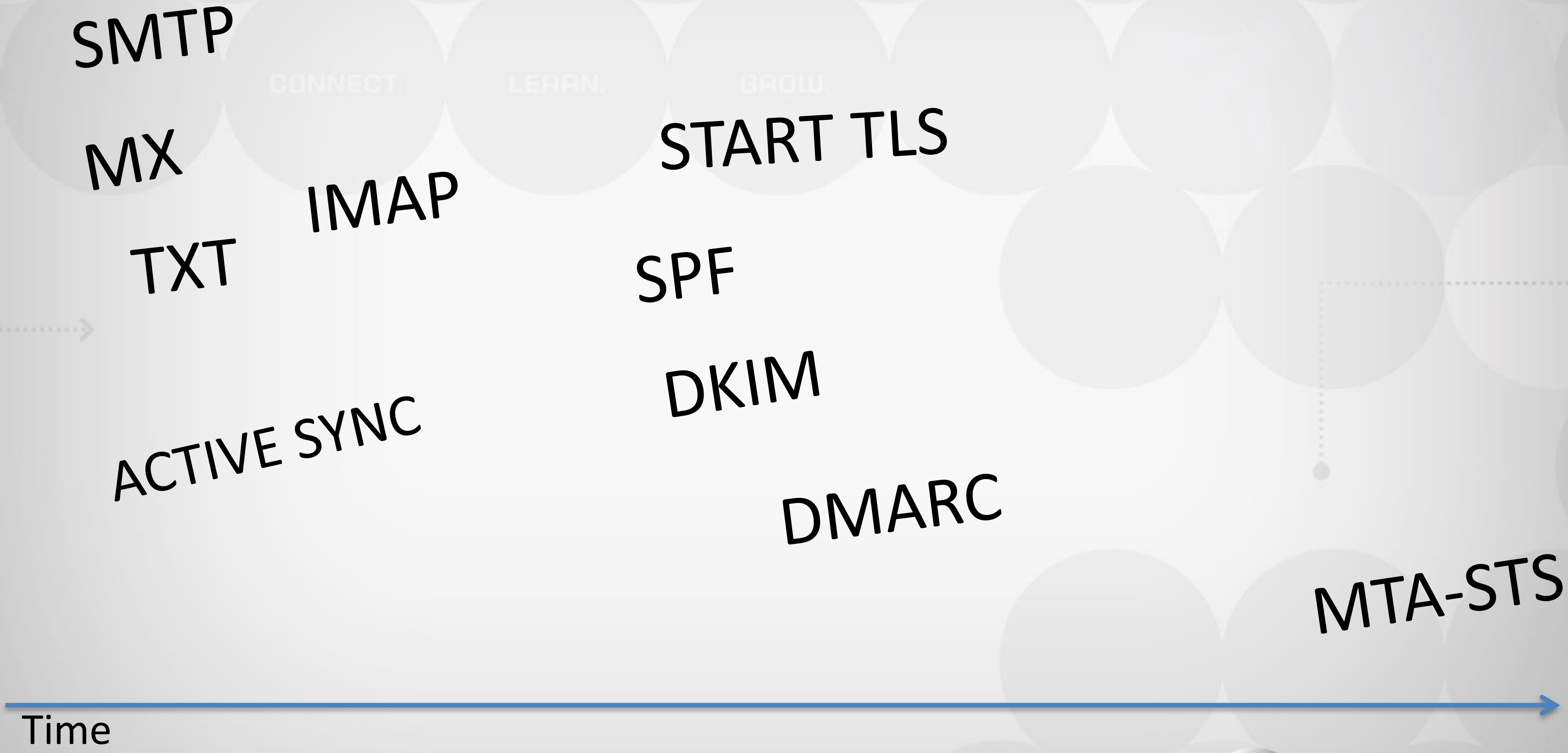
OWASP
Open Web Application
Security Project

Secure your email

ISO model for messageing (X.400)



Concepts



SMTP

MX

TXT

ACTIVE SYNC

IMAP

START TLS

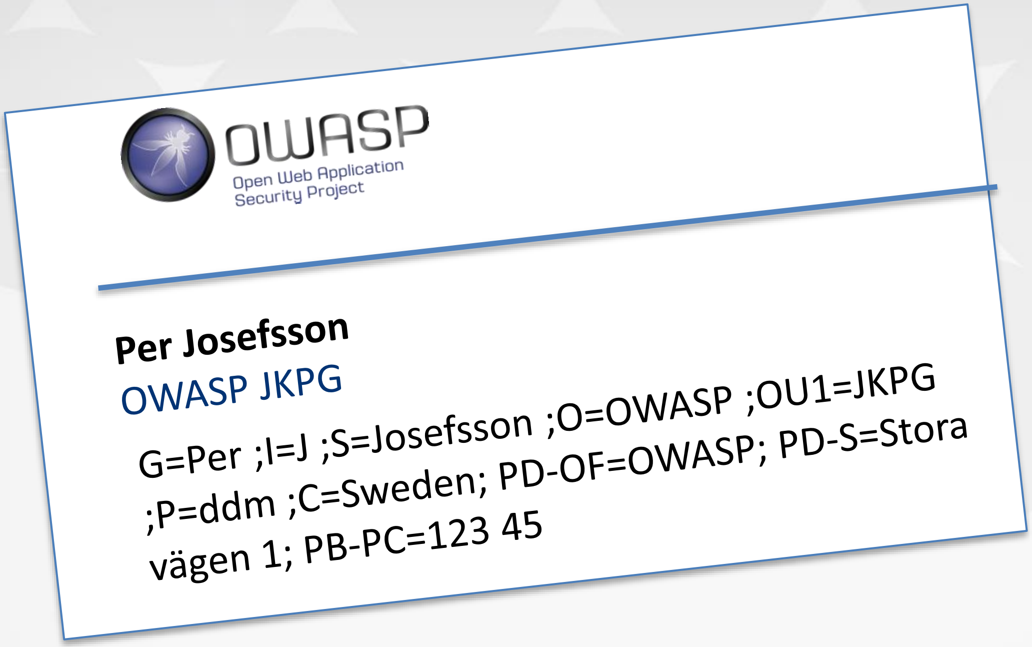
SPF

DKIM

DMARC

MTA-STS

Time



OWASP
Open Web Application
Security Project

Per Josefsson
OWASP JKPG

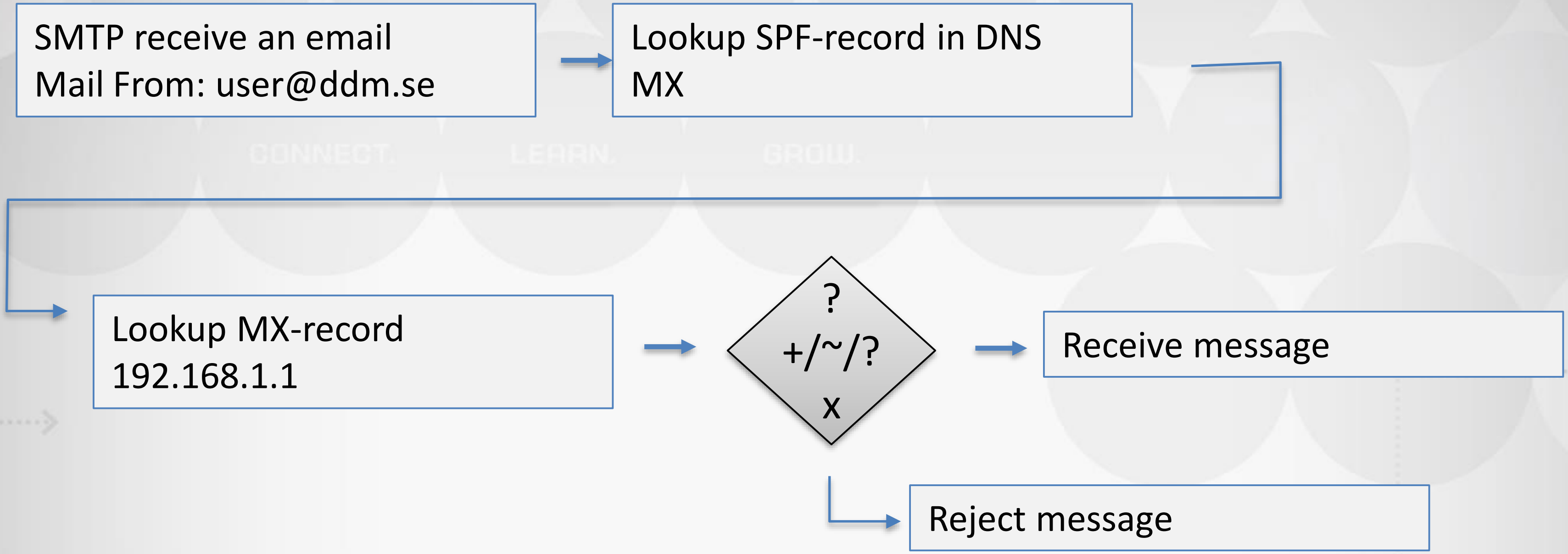
G=Per ;I=J ;S=Josefsson ;O=OWASP ;OU1=JKPG ;P=ddm ;C=Sweden; PD-OF=OWASP; PD-S=Stora vägen 1; PB-PC=123 45

SMTP

```
STARTTLS
S: 220 smtp.example.com ESMTP Postfix
C: EHLO relay.example.com
S: 250-smtp.example.com, I am glad to meet you
S: 250 SIZE 65536
C: MAIL FROM:<charlie@evil.com>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.com>
C: To: Alice Example <alice@example.com>
C: Date: Tue, 15 Jan 2008 16:02:43 -0500
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye {The server closes the connection}
```

Panasonic
SPAM

SPF



SMTP receive an email
Mail From: user@ddm.se

Lookup SPF-record in DNS
MX

Lookup MX-record
192.168.1.1

Receive message

Reject message

```
v=spf1 ip4:192.0.2.0/24 mx include:smarter.se -all
```

SPF RR syntax

Operators

+ (implicit)

-

~

?

Directives

all

mx

include

a

ipv4

ipv6

ptr

exists

redirect

exp

SPF parent & child

Example 2: SPF in alignment (parent):

MAIL FROM: <sender@child.example.com>

From: sender@example.com

Date: Fri, Feb 15 2002 16:54:30 -0800

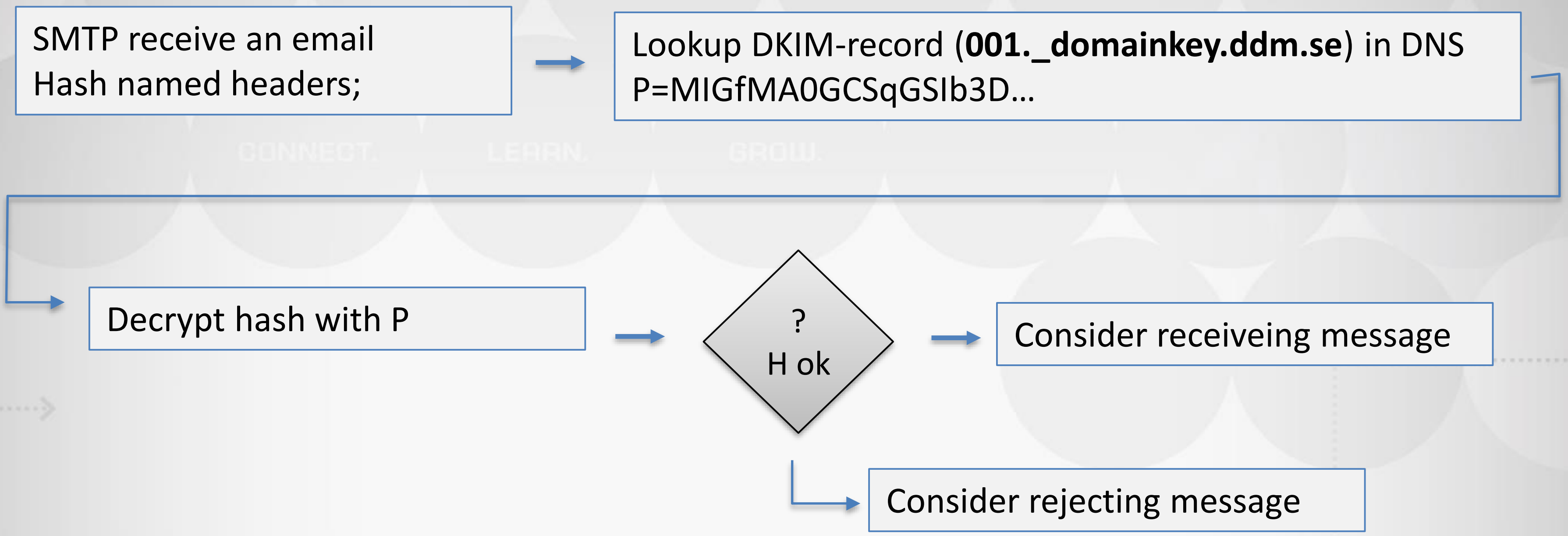
To: receiver@example.org

Subject: here's a sample

DKIM

```
Received: from [172.16.117.57] (unknown [194.236.49.11])
    (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
    (No client certificate requested)
    by ddm.se (Postfix) with ESMTPSA id 2DCFCA6DC08
    for <per.josefsson@pulsen.se>; Thu, 16 May 2019 07:40:15 +0200 (CEST)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed; d=ddm.se; s=001;
    t=1557985215; bh=BYHjJEEQX5fFwHMnm87o1Js17Fta6Hp+u/7oh9GDCQE=;
    h=From:Date:Subject:To;
    b=kSzGR6db2AIm5rCkNIXfoyngKTjaAOMFhLEEUMGXyIxr1m6SDvLtLTN1AUGZPEzb9
     LpekqkGSPqJm/8JRQ4MTbcdYcnWZT+DPRNvMI88UcO93XnVRqDCn18K5CtENhgnrjU
     NtKj7+mDiDSzUwyyrYjtB1jbCSOOZQ7usNYrHqtI=
Content-Type: multipart/mixed;
    boundary="Apple-Mail-676818E7-493B-4089-86AA-CDB76E7C7649”
From: Per Josefsson <per@ddm.se>
Date: Thu, 16 May 2019 07:40:13 +0200
```

DKIM



SMTP receive an email
Hash named headers;

Lookup DKIM-record (**001._domainkey.ddm.se**) in DNS
P=MIGfMA0GCSqGSIb3D…

Decrypt hash with P

?
H ok

Consider receiveing message

Consider rejecting message

```
v=DKIM1\; k=rsa\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5o7FC4ZpP7mis5X+9
WPfIRmUYhT+BKckUB2Q/yZ/eBOmqcTCj7tpNMHxowdbWGzLTfps08UgXbAiB+m871XQ7+V
rHU13HGKqGZU2Q0ZGu6B3KyMa0e8eSUxwVI+5V0sxQdGUctNJJP5x9CkkVT7LF6SZ3MXDa
1fl/gC5TEzDfDwIDAQAB
```

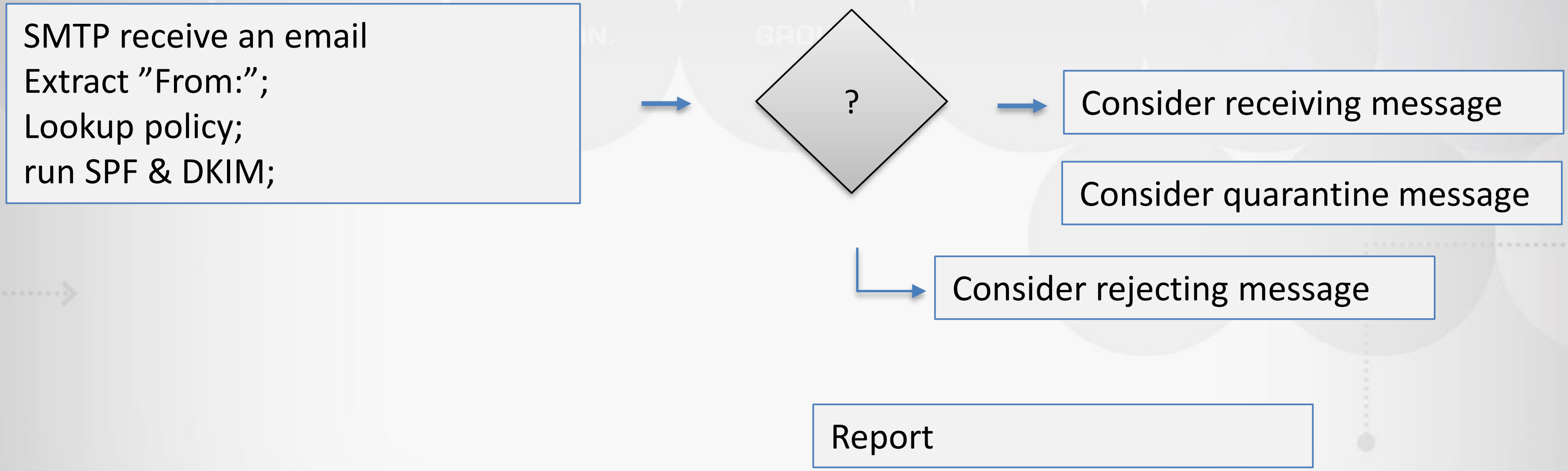
- **v**, version
- **a**, signing algorithm
- **d**, domain
- **s**, selector
- **c**, canonicalization algorithm(s) for header and body
- **q**, default query method
- **t**, signature timestamp
- **x**, expire time
- **h**, header fields - list of those that have been signed
- **bh**, body hash
- **b**, signature of headers and body

DKIM pub key lookup

```
$ nslookup
> set Q=TXT
> 001._domainkey.ddm.se
Non-authoritative answer:
v=DKIM1\; k=rsa\; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5o7FC4ZpP7mis5X+9
WPfIRmUYhT+BKckUB2Q/yZ/eBOmqcTCj7tpNMHxowdbWGzLTfps08UgXbAiB+m871XQ7+VrHU13H
GKqGZU2Q0ZGu6B3KyMa0e8eSUxwVI+5V0sxQdGUctNJJP5x9CkkVT7LF6SZ3MXDa1fl/gC5TEzDf
DwIDAQAB
```

DMARC

Domain-based Message Authentication, Reporting, and Conformance



SMTP receive an email
Extract ”From:”;
Lookup policy;
run SPF & DKIM;

?

Consider receiving message

Consider quarantine message

Consider rejecting message

Report

DMARC

```
$ nslookup
> set q=TXT
> _dmarc.ddm.se.
answer:
_dmarc.ddm.se   text = "v=DMARC1\; p=reject\;
rua=mailto:j6upbyys@ag.dmarcian-eu.com\;"
```

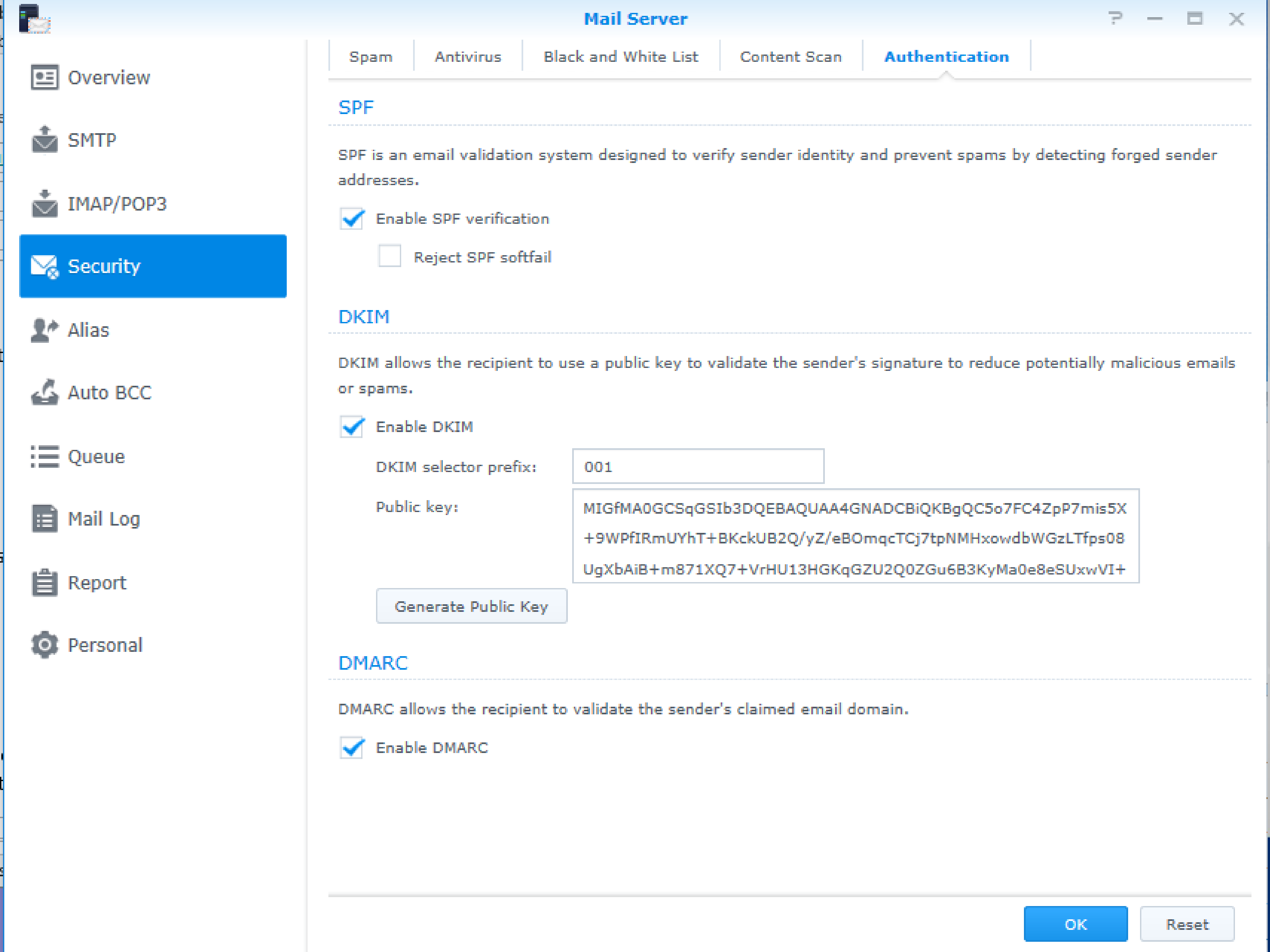
DMARC RR syntax

Tag	Value
v	Version ”DMARC1”
p	Policy ”none|quarantine|reject”
adkim	Strict or relaxed domain component for DKIM
aspf	Strict or relaxed domain component for DKIM
fo	When to report a failure ”0 (defult) | 1|d|s”
pct	% of email to enforce the policy on (default 100)
rf	Report format ”afrf (default)
ri	Report interval in seconds (default 86400)
rua	Where to send aggregate reports
ruf	Where to send forensic reports
sp	Subdomain policy ”none|quarantine|reject”

Cheat sheet

What you should do

1. Deploy DKIM & SPF. You have to cover the basics, first.
2. Ensure that your mailers are correctly aligning the appropriate identifiers.
3. Publish a DMARC record with the “none” flag set for the policies, which requests data reports.
4. Analyze the data and modify your mail streams as appropriate.
5. Modify your DMARC policy flags from “none” to “quarantine” to “reject” as you gain experience.



SPF

SPF is an email validation system designed to verify sender identity and prevent spams by detecting forged sender addresses.

☑ Enable SPF verification

□ Reject SPF softfail

DKIM

DKIM allows the recipient to use a public key to validate the sender's signature to reduce potentially malicious emails or spams.

☑ Enable DKIM

DKIM selector prefix: 001

Public key:

```
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5o7FC4ZpP7mis5X
+9WPfIRmUYhT+BKckUB2Q/yZ/eBOmqcTCj7tpNMHxowdbWGzLTfps08
UgXbAiB+m871XQ7+VrHU13HGKqGZU2Q0ZGu6B3KyMa0e8eSUxwVI+
```

DMARC

DMARC allows the recipient to validate the sender's claimed email domain.

☑ Enable DMARC

STARTTLS

STARTTLS

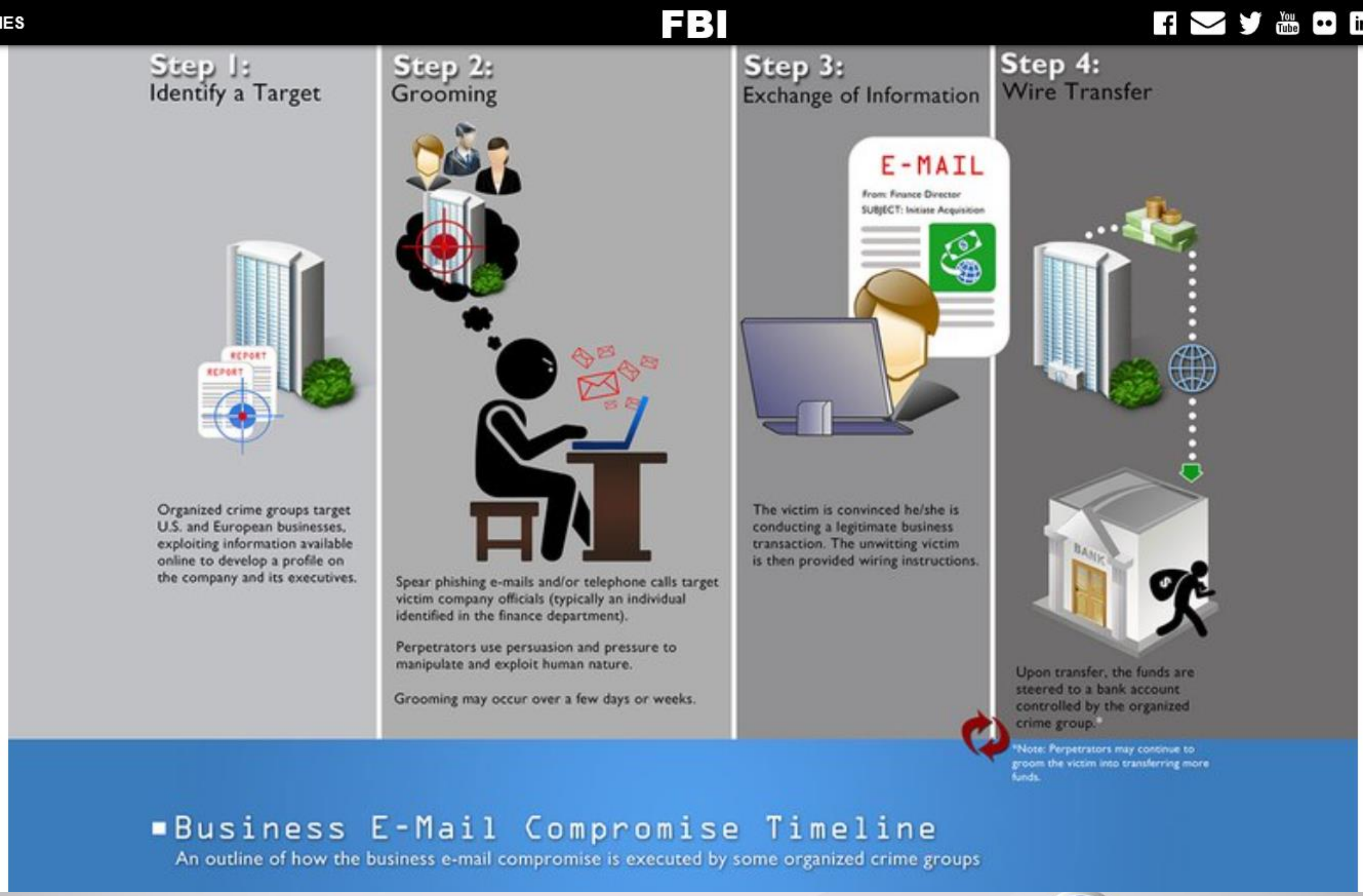
```
S: 220 smtp.example.com ESMTP Postfix
C: EHLO relay.example.com
S: 250-smtp.example.com, I am glad to meet you
S: 250 SIZE 65536
C: MAIL FROM:<charlie@evil.com>
S: 250 Ok
```

STARTTLS Everywhere

MTA-STS

https://mta-sts.ddm.se/.well-known/mta-sts.txt

```
_mta-sts.ddm.se.   300   IN   TXT
    "v=STSv1; id=aca9f86d663;"
```



Step 1:
Identify a Target

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2:
Grooming

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3:
Exchange of Information

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4:
Wire Transfer

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

▪Business E-Mail Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups

Extra